| Form PTO 1449        | ATTY                  | ATTY. DOCKET NUMBER   |         |                     | Number                       |               | P  |              |  |
|----------------------|-----------------------|-----------------------|---------|---------------------|------------------------------|---------------|--|--------------|--|
| 101                  |                       | NITT.0027             |         |                     | SERIAL NUMBER To Be Assigned |               |  |              |  |
| U.S. De              | epartment of Commerce |                       | APPL    | ICANT               |                              |               |  | S            |  |
| Patent               | and Trademark Office  |                       | KA      | MINAGA              | et al                        |               |  | <u> </u>     |  |
|                      |                       |                       |         | IG DATE             |                              | GROUP         | 212  | ر<br>ب       | <b>三二</b>  |
| Information Dis      | Con                   | Concurrently Herewith |         |                     | 2132 58                      |               |  |              |  |
| <del></del>          | <del></del>           |                       |         | .S. Patent          | Documents<br>NAME            |               | <del>-                                    </del> |              |  |
| Examiner             | Examiner DOCUMENT DAT |                       |         | l .                 | CLASS                        | SUBC          | FILING   | DATE         |  |
| Initial              | Number                |                       |         | <del></del>         |                              |               | LASS   |              |  |
|                      | <del></del>           |                       |         | <del></del>         |                              |               | <del>  </del>                                    |              |  |
|                      | <del></del>           |                       |         | <del></del>         |                              |               | <del>  </del>                                    |              |  |
|                      | +                     |                       |         | <del></del>         |                              |               | <del>                                     </del> |              |  |
|                      | <del> </del>          |                       |         | <del> </del>        | <del></del>                  |               | <del>                                     </del> |              |  |
|                      | +                     |                       |         | <del></del>         |                              |               |  |              |  |
|                      |                       |                       |         | Foreign P           | ratent Documents             | <del></del>   | <u></u>  |              |  |
| Examiner             | Document Num          |                       |         |                     |                              | CLÁS          | SUB-   | TRANS        | SLATION  |
| Initial              | DOCUMENT NUMI         | DOCUMENT NUMBER       |         | FILING DATE COUNTRY |                              | S             | CLASS  | Yes          | No   |
|                      |                       | -+                    |         |                     | <del></del>                  |               | <del>                                     </del> | 165          | 1.0  |
| <del></del>          |                       | -+                    |         |                     | <del> </del>                 |               | 1  | <del></del>  | <del>                                     </del> |
| <del></del>          | _                     | -                     |         |                     |                              | _             | +  |              | <del>                                     </del> |
| <del></del>          |                       | -                     |         |                     |                              |               | 1  |              |  |
| <del></del>          |                       | <u></u>               |         |                     |                              |               | 1  |              |  |
| L                    | Ot                    | her Do                |         | Cocluding           | g Author, Title, Date        | Pertinent P   | ages. Etc.                                       | 1            | <del></del>                                      |
| MP                   | Smart Card Ha         |                       |         |                     | , rumon, man,                |               | шдо,   |              |  |
|                      |                       |                       |         |                     | nper Resistance A            | Cautionary    | Note", T   | he Second Uf | SENIX  |
|                      | Workship on !         | Electro               | nic Com | merce Pro           | ceedings, Oakland, C         | California, I | Nov. 18-2  | 1, 1996, pp. | 1-11   |
| <del>-     -  </del> |                       |                       |         |                     | acques Quisquater, "         |               |  |              |  |
|                      |                       |                       |         |                     | Journal of Cryptolo          |               |  |              | , ,  |
| <del>-  / </del>     |                       |                       |         |                     | ation Without Trial I        |               |  | ics of Compu | tation,  |
| V                    | Volume 44, N          |                       |         |                     |                              |               |  | -            |  |
|                      |                       |                       |         |                     |                              |               |  |              |  |
|                      |                       |                       |         |                     |                              |               |  |              |  |
|                      |                       |                       |         |                     | <del></del>                  |               |  |              |  |
|                      |                       |                       |         |                     |                              |               |  |              |  |
|                      |                       |                       |         |                     |                              |               |  |              | <del></del>                                      |
|                      |                       |                       |         |                     |                              |               |  |              |  |
|                      |                       |                       |         |                     |                              |               |  |              | _  |
|                      |                       |                       |         |                     |                              |               |  |              |  |
|                      |                       |                       |         |                     |                              |               |  |              |  |
|                      | 1                     |                       |         |                     |                              |               |  |              |  |
|                      |                       |                       |         |                     |                              |               |  |              |  |

EXAMINER: Initial if citation is considered, whether or not citation is in conformance with MPEP 609; draw a line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant

| O E. JC,    | <b>*</b> .<br>병  | . •                 |               |
|-------------|--|---------------------|---------------|
| JUL 1 6 ZU  |  | ATTY. DOCKET NUMBER | SERIAL NUMBER |
| / 105       | Figur PTO 1449   | NITT.0027           | 09/931,937    |
| PREMI & TRA | Form PTO 1449  U.S. Department of commerce Patent and Trademark Office | APPLICANT           |               |
|             |  | KAMINAGA et al.     |               |
|             | Information Disclosure Statement by Applicant                          | FILING DATE         | GROUP         |
|             |  | August 20, 2001     | 2132          |

U.S. Patent Documents

| Examiner<br>Initial | DOCUMENT NUMBER | DATE     | NAME          | CLASS | SUB-<br>CLASS | FILING DATE |
|---------------------|-----------------|----------|---------------|-------|---------------|-------------|
| ИD                  | 6,049,613       | 04/11/00 | Jakobsson     |       |               | 01/13/98    |
| ид                  | 5,631,960       | 05/20/97 | Likens et al  |       |               | 08/31/95    |
|                     |                 |          | <del>- </del> |       |               |             |
|                     |                 |          | <b>†</b>      |       | <del> </del>  |             |

Foreign Patent Documents

| Examiner<br>Initial | DOCUMENT NUMBER | •                  | FILING DATE | COUNTRY | CLASS        | SUB-<br>CLASS | TRANSLATION |              |
|---------------------|-----------------|--------------------|-------------|---------|--------------|---------------|-------------|--------------|
|                     |                 | ·                  |             |         |              | YES           | No          |              |
| 110                 |                 | WO 99/67919        | 06/03/99    | PCT     |              |               | Х           |              |
|                     |                 |                    |             |         |              | REC           | EIVI        | D            |
|                     | -               |                    |             |         |              | JUL           | 1 6 200     | 3            |
|                     |                 |                    |             |         |              | echnolo       | gy Cente    | <u> 2100</u> |
|                     |                 | - <del>10-12</del> |             |         |              |               |             |              |
|                     |                 |                    |             |         |              |               |             |              |
| _                   |                 |                    |             |         | <del> </del> |               |             |              |

Other Documents (Including Author, Title, Date Pertinent Pages, Etc.) Ramesh Karri, Kaijie Wu, Piyush Mishra, Yongkook Kim, "Concurrent Error Detection of Fault-Based Side-Channel Cryptanalysis of 128-Bit Symmetric Block Ciphers", Proceedings of MO the 38th Annual Design Automation Conference, June 18-22, 2001, Proceedings of the Design Automation Conference, New York, pp. 579-584 Dan Boneh, Richard A. DeMillo, Richard J. Lipton, "On the Importance of Checking MP Cryptographic Protocols for Faults", Advances in Cryptology - Eurocrypt '97, International Conference on the Theory and Application of Cryptographic Techniques Proceedings, 1997, pp. 37-51 Mn European Search Report dated June 30, 2003.

**EXAMINER** 

11/02/04 **DATE CONSIDERED** 

Examiner: Initial if citation is considered, whether or not citation is in conformance with MPEP 609; draw a line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant

PTO 1449